

# Multilevel Encryption integrated with Image Steganography for secure data transmission

Mr.Suryawanshi A.M.<sup>1</sup> Miss.Jagatap P.S.<sup>2</sup> Sakshi Ingale<sup>3</sup> Vaishnavi Somase<sup>4</sup>

<sup>1,2,3,4</sup>Department of Information Techonology, Dattakala Group of institute Swami Chincholi, Pune, Maharastra, India

**Abstract:** *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.*

**Keywords:** Image steganography, steganalysis, hiding capacity, imperceptibility, security.

## I.INTRODUCTION

Image steganography is the art and science of concealing secret information within digital images, ensuring that the hidden data remains imperceptible to the human eye. This technique has evolved significantly, especially with the integration of artificial intelligence (AI), enhancing both the capacity and security of data hiding methods.

At its core, image steganography involves embedding hidden messages—be it text, images, or files—into a cover image. The most common method is Least Significant Bit (LSB) substitution, where the least significant bits of pixel values are altered to encode the secret data. This modification is subtle enough that the resulting image appears identical to the original to the naked eye.

## II. LITERATURE SURVEY

| Sr. No | Title of paper                                                                                                         | Author                                                           | Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | Image Steganography: A Review of the Recent Advances                                                                   | Nandhini Subramanian <sup>1</sup> , Omar Elharrouss <sup>1</sup> | To explore and discuss various deep learning methods available in image steganography field. Deep learning techniques used for image steganography can be broadly divided into three categories traditional methods, Convolutional Neural Network-based and General Adversarial Network-based methods. Along with the methodology, an elaborate summary on the datasets used, experimental set-ups considered and the evaluation metrics commonly used are described in this paper. |
| 2      | A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network | Xintao Duan <sup>1</sup> , Daidou Guo                            | We propose a new high capacity image steganography method based on deep learning. The Discrete Cosine Transform is used to transform the secret image, and then the transformed image is encrypted by Elliptic Curve Cryptography to improve the anti-detection property of the obtained image. To improve steganographic capacity, the SegNet Deep Neural Network with a set of Hiding and Extraction networks enables steganography and extraction of full-size images.           |

|    |                                                                               |                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. | Reversible Image Steganography Scheme Based on a U-Net Structure              | XINTAO DUAN <sup>1</sup> , KAI JIA <sup>1</sup> , BAOXIA LI <sup>1</sup> ,  | We propose a new image steganography scheme based on a U-Net structure. First, in the form of paired training, the trained deep neural network includes a hiding network and an extraction network; then, the sender uses the hiding network to embed the secret image into another full-size image without any modification and sends it to the receiver.                                                                                                                                                                                                                                                                                         |
| 4. | Detection of Image Steganography Using Deep Learning and Ensemble Classifiers | Mikołaj Plachta, Marek Krzemie'n , Krzysztof Szczypiorski and Artur Janieki | The problem of detecting JPEG images, which have been steganographically manipulated, is discussed. The performance of employing various shallow and deep learning algorithms in image steganography detection is analyzed. The data, images from the BOSS database, were used with information hidden using three popular steganographic algorithms: JPEG universal wavelet relative distortion (J-UNIWARD), nsF5, and uniform embedding revisited distortion (UERD) at two density levels. Various feature spaces were verified, with the discrete cosine transform residuals (DCTR) and the Gabor filter residuals (GFR) yielding best results. |

### III. OBJECTIVE

- To explore techniques of hiding data using encryption module of this project To extract techniques of getting secret data using decryption module.
- Steganography refers to the practice of concealing a message (with no traceability) in a manner that it will make no meaning to anyone else except the intended recipient, while cryptography, on the other hand, refers to the art of converting a plaintext (message) into an unreadable format.
- The purpose of audio steganography is to cover confidential data in digital audio for

confidentiality. To embed the secret image into the audio signal is the objective of the proposed audio steganography

### IV. TOOLS AND TECHNOLOGY

Due to Software project we use embedded python SOFTWARE DESCRIPTION

OpenStego: This program is an open-source steganography tool. Xiao Steganography: Xiao hides secret files in WAV or BMP files. Crypture: This application is a command-line tool used to conduct steganography. NoClue: This application is an open-source tool that hides text information in both video and image carrier.

### V. ACTIVITY DIAGRAM

#### 5.1 ACTIVITY DIAGRAM:

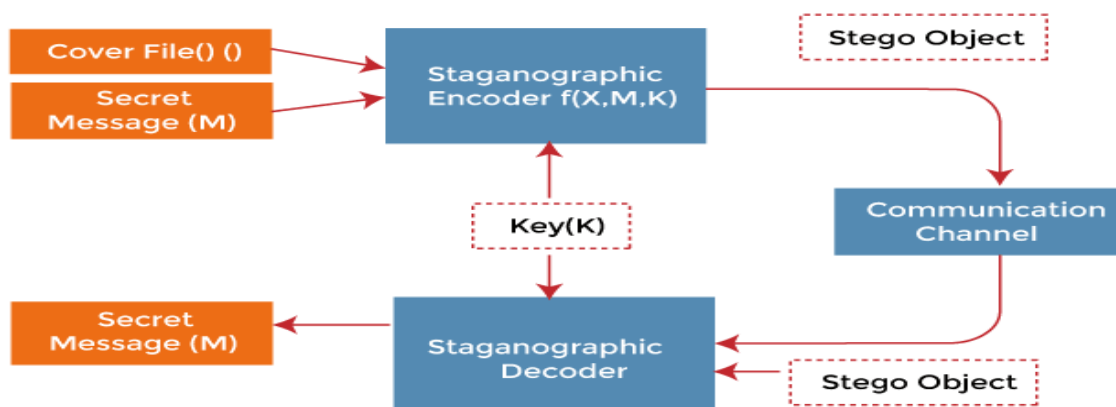



FIG. ACTIVITY DIAGRAM

5.2 Output:

10:27

Welcome to ChatBud



Read out Privacy Policy. Tap "Accept and continue" to accept the Terms of Service.

NEXT

10:28

Verify +91+917057009585

Sit Back and Relax! While we verify your phone number.  
(Enter the OTP below in case if we failed to detect SMS automatically.)


Enter OTP here

VERIFY OTP

10:27

Welcome to ChatBud

ChatBud Will send you a SMS message to verify your phone number. Please enter your contry code and phone number.

 (IN) +91 -


Carrier SMS charges may apply.

GET OTP

10:29

Profile info

Please provide your name and an optional profile photo.



Type your name here

About

NEXT



### Invite Your Friends

None of your contacts use ChatBud.  
Use the button below to invite them.

INVITE A FRIEND

CHOOSE IMAGE

Message -

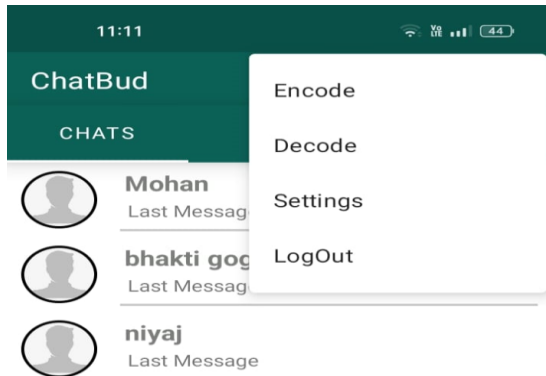
Enter message

Secret Key -

Enter secret key

ENCODE

SAVE IMAGE



CHOOSE IMAGE

Message -

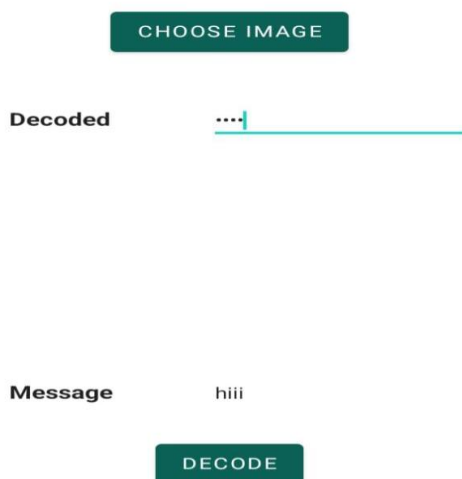
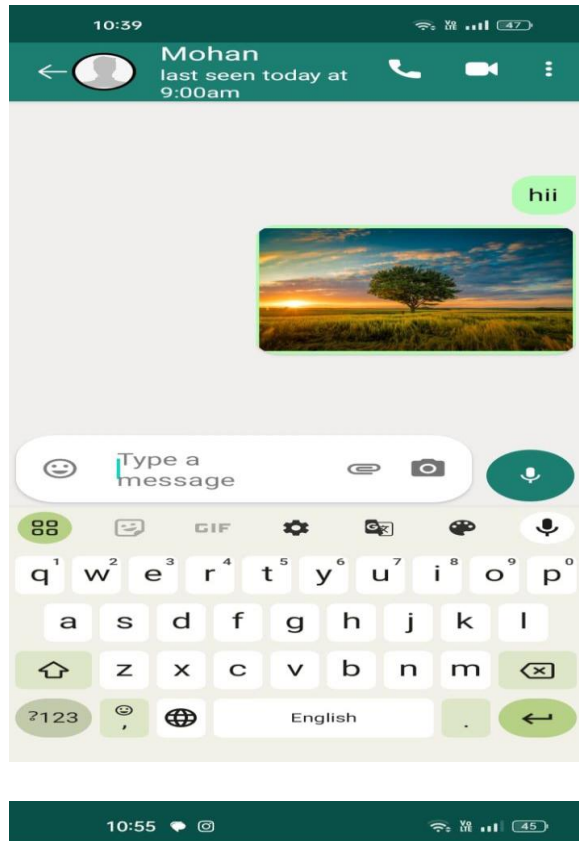
Hello

Secret Key -



ENCODE

SAVE IMAGE



## VI. ADVANTAGES AND APPLICATIONS

### 6.1 Advantages:

Difficult to detect, only receiver can detect.

Can be applied differently in digital image file.

6.2 Applications: This system can be used by the multiple peoples to get the counselling sessions online

## VII. CONCLUSION AND FUTURE SCOPE

### CONCLUSION

This paper discards the information embedding of the least significant bits of the image, but uses an end-to-end approach to hide one image onto another and has lower pixel distortion. Experimental results show that this method has significant advantages in both visual effect and steganography capacity. The next step in this paper will combine the process of image delivery with the generative adversarial networks, taking the form of passing image parameters to the receiver. The receiver extracts the transmitted secret image through the pre-trained model, and in the form of double encryption, ensures that the secret message cannot be detected by the attacker during the transmission process, and the information is secure.

### FUTURE SCOPE

Machine Learning Integration: Future steganography techniques may be Advanced Encryption Techniques: As computing power increases, more sophisticated encryption techniques may be developed to enhance the security of hidden messages within images. This could involve quantum-resistant algorithms or other cutting-edge cryptographic methods.

Average machine learning algorithms for both embedding and detecting hidden information. These algorithms could adapt to evolving detection methods, making it more challenging to identify steganographic content.

## REFERENCE

- [1] Wikipedia. (2020). Steganography. [Online]. Available: <https://en.wikipedia.org/wiki/Steganography>.
- [2] H. Shi, X.-Y. Zhang, S. Wang, G. Fu, and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning," in Proc. Int. Conf. Comput. Sci. Cham,

- Switzerland: Springer, 2019, pp. 31\_x0015\_43.
- [3] M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. Srikanth, and M. Reddy, ``Digital video steganography using LSBtechnique," Red, vol. 100111, Apr. 2020, Art. no. 11001001.
  - [4] S. S. M. Than, ``Secure data transmission in video format based on LSB and Huffman coding," Int. J. Image, Graph. Signal Process., vol. 12, no. 1, p. 10, 2020.
  - [5] M. B. Tuieb, M. Z. Abdullah, and N. S. Abdul-Razaq, ``An efficiency, secured and reversible video steganography approach based on lest significant," J. Cellular Automata, vol. 16, no. 17, Apr. 2020.
  - [6] H. M. Sidqi and M. S. Al-Ani, ``Image steganography: Review study," in Proc. Int. Conf. Image Process., Comput. Vis., Pattern Recognit. (IPCVP), 2019, pp. 134\_x0015\_140.